ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ТҰҢҒЫШ ПРЕЗИДЕНТІ - ЕЛБАСЫНЫҢ ҚОРЫ

«ҒЫЛЫМ ЖӘНЕ БІЛІМ – 2017»

студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ – 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«SCIENCE AND EDUCATION - 2017»

14th April 2017, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

«Ғылым және білім - 2017»
студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«Science and education - 2017»

2017 жыл 14 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2017» студенттер мен жас ғалымдардың XII Халықаралық ғылыми конференциясы = The XII International Scientific Conference for students and young scholars «Science and education - 2017» = XII Международная научная конференция студентов и молодых ученых «Наука и образование - 2017». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2017. – 7466 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-827-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-827-6

2-е изд., перераб. И доп. – СПб: БХВ-Петербург, 2016. -256 с.: ил.-(Электроника)
5. https://processing.org/overview/
6. Farrell J. Java Programming – Course Technology: 2015-1026p.
7. http://fritzing.org/home/

УДК 04.056

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕРВИСА АУТЕНТИФИКАЦИИ WEB-ПРИЛОЖЕНИЙ

Мансуров Акылбек Мухамедхалиевич,
mansurov.akylbek@gmail.com
магистрант 1-го курса факультета информационных технологий ЕНУ им. Л.Н. Гумилева,
Астана, Казахстан
Научный руководитель – Сатыбалдина Д.Ж.

В настоящее время интерактивные web-приложения являются важной частью информационных систем самого разного назначения. Основной особенностью таких систем является организация доступа клиентов к Интернет ресурсам, при этом пользователи должны однозначно аутентифицировать себя. Существует множество способов организации процесса аутентификации пользователей, из которых чаще всего используется аутентификация с помощью форм [1]. В то же самое время разрабатывается множество инструментов для организации атак на сайты, с целью получения несанкционированного доступа к web приложению и ресурсам. Многие из этих инструментов используют автоматизированные процедуры преодоления процессов аутентификации web-приложений посредством использования ботов. Бот – это программное обеспечение робота, экземпляр вредоносного программного обеспечения, работающий на зараженном компьютере автономно и автоматически без ведома пользователя [2]. Соответственно в задаче аутентификации возникает проблема определения того, кем является пользователь: человеком или компьютером, ботом.

Для решения данной проблемы разработчики веб-сервисов используют системы, основанные на реализации теста Тьюринга. Основная идея теста: предложить пользователю такую задачу, которую может решить человек, но которую несоизмеримо сложно или невозможно решить компьютеру. Такого рода задачи называются CAPTCHA, где CAPTCHA – это акроним от англоязычного выражения "Completely Automated Public Turing test to tell Computers and Humans Apart" (что в переводе на русский язык означает: "Полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей") [3].

Однако, CAPTCHA не является абсолютно идеальным методом защиты, так как с развитием алгоритмов генерации CAPTCHA, развиваются и методы распознавания или обхода подобных систем. В этой связи являются актуальными исследования направленными на является усовершенствование методов обеспечения безопасности веб-сервисов, использующих системы генерации CAPTCHA. В настоящей работе представлен аналитический обзор существующих решений на основе CAPTCHA систем, выделены основные требования по обеспечению безопасности веб-сервисов, приведены направления использования, достоинства и недостатки различных вариантов реализации.

Выделяют 3 основные характеристики, которым должна удовлетворять качественная CAPTCHA [4]:

- тест должен быть простым для человека;
- тест должен быть простым для генерации и оценки тестирующей машиной;
- тест должен быть сложным для автоматизированных ботов.

В настоящее время сфера применения CAPTCHA расширена, она используются для:

- предотвращения выполнения автоматизированным программным обеспечением

действий, которые понижают качество обслуживания веб-сервисами;
- минимизирования количества автоматических сообщений на различных сайтах;
- предотвращения спам-сообщений в блогах;
- защиты регистрации на веб-сайтах;
- защиты Email адресов;
- защиты от Scraper'ов;
- онлайн опросов, когда IP адреса проголосовавших записываются, с целью предотвращения многократного голосования одним пользователем;
- предотвращения атак, использующих словари;
- поисковых роботов, когда предпочтительно оставлять веб-страницы не проиндексированными, чтобы люди не смогли так просто их найти;
- предотвращения распространения червей и спама [5].

Существуют различные виды CAPTCHA. Некоторые из них представлены ниже [6]:

1) CAPTCHA, основанные на тексте;
2) CAPTCHA, основанные на изображениях;
3) CAPTCHA, основанные на аудио;
4) CAPTCHA, основанные на вопросах.

Рассмотрим подробнее каждый вид CAPTCHA.

1. CAPTCHA, основанные на тексте. Данные CAPTCHA используют цифры и буквы алфавита. К сгенерированному изображению с текстом добавляются шум и искажения, с целью предотвращения атак ботов. Выделяют несколько характеристик для текста:

- шрифт и размер текста;
- группа символов, т.е. коллекция символов используемых в CAPTCHA;
- искажение, т.е. изменение изображения путем изменения относительного расположения пикселей;
- наклон, имеется в виду наклон символов под разными углами;
- размазывание, относится к позиционированию наклоненных символов в различных вертикальных местах, создавая волновую картину с текстовым передним планом.

В работе [7] представлены CAPTCHA, основанные на времени, и CAPTCHA, основанные на предложения, как два подвида CAPTCHA, основанной на тексте. В CAPTCHA, основанных на времени, пользователь должен вводить символы, которые появляются через короткие промежутки времени, в различных областях экрана, в порядке в котором они появляются. Эта CAPTCHA заканчивается, если тестирующая машина не получает ответ в определенный промежуток времени. Идея состоит в том, что человек способен решить данное испытание быстро, но компьютеру для решения требуется некоторое время. В CAPTCHA, основанных на предложениях, после выбора двух случайных слов из предложения они перемешиваются. Затем пустые места предложения заполняются случайными значениями алфавита. Пользователь должен написать предложение в правильном формате.

Интересным методом CAPTCHA, основанной на тексте, является reCAPTCHA, пример которой представлен на рисунке 1. reCAPTCHA – это система, используемая одновременно для защиты веб-сервисов от интернет-ботов и для оцифровки текстов книг [5]. reCaptcha широко используется такими web-приложения как Facebook, TicketMaster, Twitter, Bash.org.ru и StumbleUpon. Кроме того, она позволяет использовать полученные результаты для распознания различной литературы, предназначенной для оцифровки.

Рисунок 1 – Пример reCAPTCHA

2. CAPTCHA, основанные на изображениях. Существует множество CAPTCHA данного типа. Пример одной из них приведен на рисунке 2. Однако, большая их часть показывает пользователям группу изображений из базы данных CAPTCHA. Множество из старых CAPTCHA, использующих изображения, имели ограниченную базу данных с изображениями, где хранились сами изображения вместе с их тегами. Данный подход имеет несколько проблем безопасности. Например, ограниченный объем базы данных позволяет атакующему, со временем, выучить всю базу данных и затем получить доступ к системе. Кроме того, при таком подходе, для обеспечения безопасности, базы данных с изображениями и тегами должны быть конфиденциальными, что противоречит принципу Кирхгоффа, который гласит, что система безопасности должна оставаться безопасной, даже если алгоритмы и базы данных находятся в публичном доступе. Некоторые другие решения предполагают включение семантики в CAPTCHA. Семантика – это человеческие способности к распознаванию определенных субъектов на картине [3]. Преимуществом CAPTCHA, основанной на изображениях, является то, что распознавание образов является трудной задачей ИИ, поэтому трудно взломать данный тест, используя методики распознавания [6].

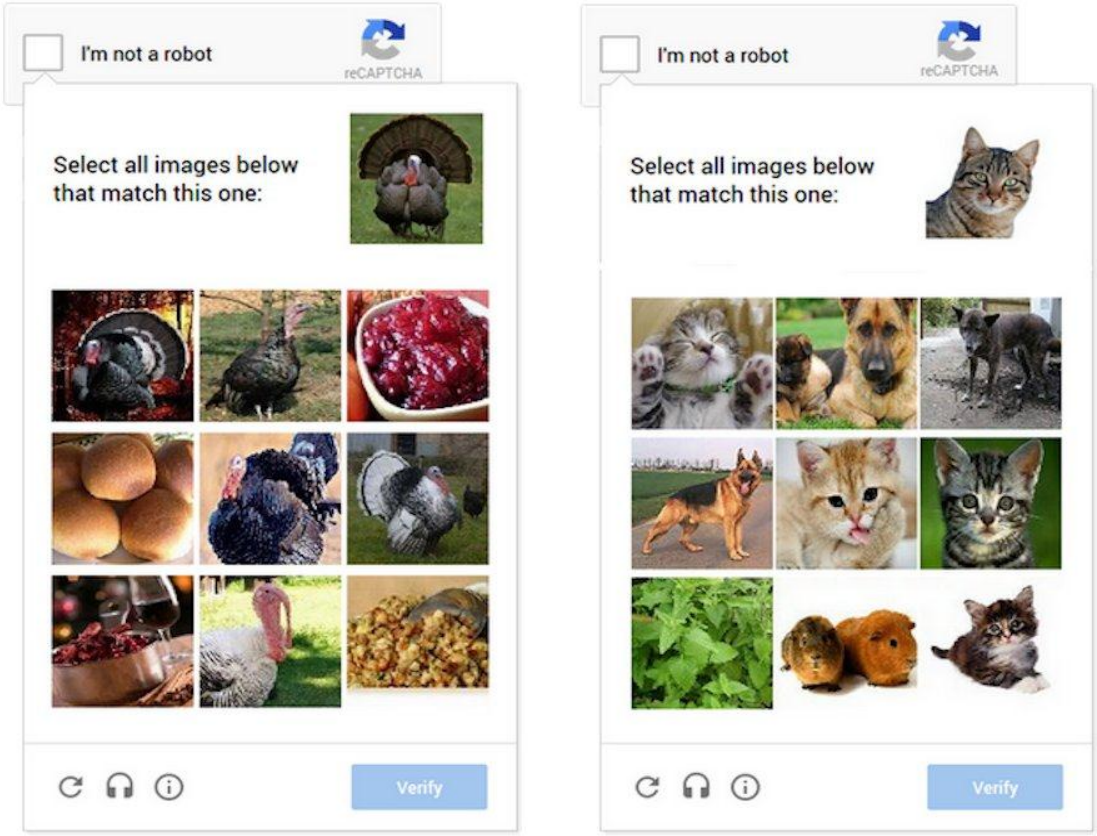

Рисунок 2 - Пример Google reCAPTCHA

3. CAPTCHA, основанная на аудио. Тест проигрывает аудио, который содержит запись искаженного слова или последовательности цифр, после чего пользователю необходимо ввести услышанное сообщение (см. рисунок 3). Предыдущие исследования со слепыми пользователями показали, что в данный тест не очень пригоден, т.к. процент успешного выполнения составляет менее 50%. Данная проблема указывает на необходимость новых подходов, которые обеспечивают большее удобство использования, при этом, не жертвуя безопасностью [8].

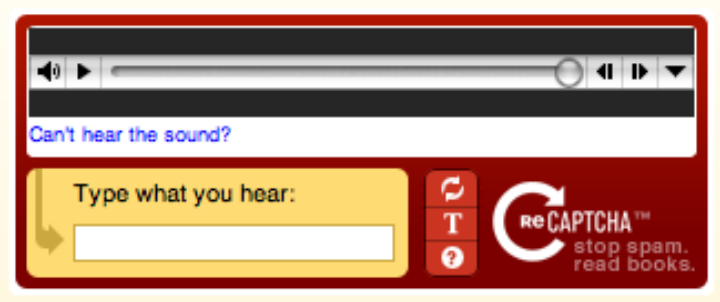

Рисунок 3 - Пример CAPTCHA основанной на аудио.

4. CAPTCHA, основанные на вопросах. В данном типе CAPTCHA пользователю задаются простые вопросы или математические тесты. В подобных тестах, согласно предопределенному математическому шаблону генерируется простая математическая проблема. Затем тест сохраняется и показывается пользователю в форме изображения. Для решения данного теста необходимо четыре способности: понимание текста вопроса, определение вопросительных изображений, понимание проблемы, решение проблемы. Тест легко может быть решен человеком, т.к. он хочет только запомнить ответ, что требует немного времени. Для интернет-бота проблема состоит в том, что он должен распознать фразу, размер, форму и текст изображения. Даже, в том случае, если он получит все вышеуказанные данные, он должен быть способен ответить на указанный вопрос [7].

В таблице 1 на основе анализа различных методы защиты web-приложения от ботов приведены преимущества и недостатки данных методов.

Таблица 1. Достоинства и недостатки различных типов CAPTCHA

Тип CAPTCHA	Достоинства	Недостатки
CAPTCHA, основанные на тексте	Как правило, самый быстрый и простой способ определения (аутентификации) пользователя	Относительно других типов CAPTCHA, легко взламывается, с помощью технологий OCR (англ. optical character recognition – Оптическое распознавание символов)
CAPTCHA, основанные на изображениях	Преимуществом данного типаCAPTCHA, является то, что распознавание образов является трудной задачей ИИ, поэтому трудно взломать данный тест, используя методики распознавания [6]	Некоторые пользователи сталкиваются с проблемой идентификации изображения, вследствие того, что имеют плохое зрение, либо изображение слишком плохого качества
CAPTCHA, основанные на аудио	Данный тип теста могут проходить пользователи с плохим зрением либо вовсе слепые пользователи	Чаще всего тесты представлены на английском языке, отсюда следует что, конечный пользователь должен обладать

		знанием английского языка. Сложно определять слова схожие по звучанию
CAPTCHA, основанные на вопросах	В зависимости от вопросов, тест может быть простым и не требует много времени от пользователя	Не является устойчивым к взлому, так как простые математические задачи легко решаются компьютером, а при использовании логических вопросов требуется большая база вопросов

Результаты анализа стойкости существующих решений, их соответствие современных требованиям, показало, что необходимо использовать комбинированные методы из нескольких видов CAPTCHA одновременно, включая визуальные и звуковые системы. При этом, следует учесть, что пользователи с некоторыми физическими недостатками (со слабым слухом или плохим зрением, с познавательными расстройствами и т.п.) могут иметь определенные трудности, используя эти системы. Разработчикам необходимо гарантировать, что пользователи с ограниченными возможностями будут иметь несколько способов взаимодействия с ресурсами сайта.

Список использованных источников

1. Коломыцев М., Носок С., Грайворонский Н. Безопасность пользовательских процедур аутентификации web-приложений // «Захист інформації». Науково-практичний журнал, НАУ, Киев.- №1(15), 2013. - С.75-80.
2. Косенко М.Ю., Мельников А.В. Вопросы обеспечения защиты информационных систем от ботнет атак //Вопросы кибербезопасности.- №4(17) - 2016.- С.20-28.
3. Mehrnezhad M. et al. PiSHi: click the images and I tell if you are a human //International Journal of Information Security. – 2016. – С. 1-17.
4. Saini B. S., Bala A. A review of bot protection using CAPTCHA for web security //IOSR Journal of Computer Engineering. – 2013. – Т. 6. – С. 36-42.
5. Azad S., Jain K. CAPTCHA: Attacks and weaknesses against OCR Technology //Global Journal of Computer Science and Technology. – 2013. – Т. 13. – №. 3.
6. Singh V. P., Pal P. Survey of Different Types of CAPTCHA //International Journal of Computer Science and Information Technologies. – 2014. – Т. 5. – №. 2. – С. 2242-2245.
7. Soumya K. R. et al. A Survey on Different CAPTCHA Techniques. – 2014.
8. Lazar J. et al. The SoundsRight CAPTCHA: an improved approach to audio human interaction proofs for blind users //Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. – ACM, 2012. – С. 2267-2276.

ӘОЖ 004.04

ЦИСТЕРНАДАҒЫ МҰНАЙ КӨЛЕМІН ӨЛШЕУДІ АВТОМАТТАНДЫРУ

Нағметулла Темірлан Еділұлы

e.nagmetulla@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті «Есептеу техникасы» кафедрасы ЕТБҚ-21 тобының студенті, Астана, Қазақстан

Ғылыми жетекшісі – А.Адамова

XXI ғасыр – жаңа технологияның, ғылым-білімнің ғасыры. Жаңа технологиялар уақыт өткен сайын қуса жеткізбестей қарқынмен дамып жатыр. Бүгін үйренген білімің ертеңгі күні жарамсыз болып қалса, таң қалуға болмайды. Ақпараттық технологиялар саласындағы